REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars:

Examiner interview

Applicant appreciates the courtesies extended to Applicant's representative during the personal interview conducted on August 29, 2006.

During the interview, Applicant's representative discussed with the examiner the Office Action of June 30, 2006.

Applicant's representative pointed out to the examiner several differences between the claimed invention and the cited reference (the Boerbert patent). In particular, it was pointed out that Boerbert never presents a secret code (data read from a data carrier or token) to the user, and therefore cannot receive from the user an indication of the correctness of the secret code. It was noted that Boerbert's "countersign" differs from the secret code of the present application in that a countersign read from the token is not displayed to the user for the user's scrutiny and indication of correctness. Instead, a countersign is displayed ***only at the end of the process*** described in Boerbert's Fig. 4, ***after*** authentication is complete (after a successful login at step 128). Thus, display of the countersign has no role in the authentication process.

Further, Applicant's representative noted that the claims clearly dictate an order for reading the secret code, presenting the secret code to a user, receiving a user's indication that the secret code is correct, and then reading a presented biometric feature.

While no specific agreement was reached regarding the claims, the examiner indicated agreement that Boerbert does not appear to teach or suggest the sequence of events of the present invention.

The examiner expressed concern that claim 1 is unclear with respect to the ordering of steps. Applicant's representative noted that certain ordering is clearly

expressed in claim 1, such as the recitation that "***after receiving*** an indication that the presented read secret code is correct, reading a biometric feature presented by the user" (emphasis added). It was noted that such recitation requires that the ***read*** secret code is presented to the user, and that an indication that the ***presented*** secret code is correct is received before the biometric feature is read.

Rejection of claims 1-9 under 35 U.S.C. § 103(a)

Claims 1-9 presently stand rejected as being unpatentable over Boerbert (U.S. 5,272,754). This rejection is respectfully traversed for at least the following reasons.

Claim 1 has been amended to clarify that it is an indication by the user that the presented read secret code is correct that is received prior to reading a biometric feature, and that the read presented biometric feature is compared with a biometric feature stored on the data carrier. Accordingly, it is respectfully submitted that claim 1 more clearly describes the sequence of steps of the present invention.

It is respectfully submitted that Boerbert fails to disclose or suggest each and every element set forth in claim 1 of the present invention.

Claim 1 describes a method for authenticating a user of a data carrier, comprising steps of reading a secret code from a data carrier, presenting the read secret code to the user, and receiving an indication by the user that the presented read secret code is correct. After the indication that the presented secret code is correct is received, a biometric feature presented by the user is read. Finally, the read presented biometric feature is compared with a biometric feature stored on the data carrier.

Boerbert fails to disclose or suggest reading a secret code from a data carrier, and then presenting the secret code to a user.

Boerbert never displays to the user any secret code read from a data carrier. Instead, it appears that a ***new*** countersign is displayed to the user, at the end of a process described in Boerbert's Fig. 4 after authentication is complete (after a successful login at step 128). "Each time a user entity 23 is identified to the Security Kernel (e.g., each new

session on processor 42), countersign generating apparatus 50 generates a fresh countersign" (*Boerbert*; col. 6, lines 48-51).

Boerbert fails to disclose or suggest accepting from a user an indication that a secret code (or countersign) is correct. According to Boerbert, the countersign is displayed ***only at the end of the process*** described in Boerbert's Fig. 4, ***after*** authentication is complete (after a successful login at step 128). At no point does the user enter any indication that the countersign is correct or incorrect, and since the countersign is displayed only after authentication is complete, there can be no teaching or suggestion that any user action is required following display of the countersign in order to complete the authentication process.

A user does not make any evaluation of the countersign, according to Boerbert's teaching. Instead, "the user enters a five digit password into authentication device 72 at 110 and, at 112, controller 66 builds a message containing the password and the user name, access authorization and ***last countersign***. This message is sent as a packet to computer-side terminator 62. Computer-side terminator 62 receives the packet and forwards it to ***computer 60 for verification***" (*Boerbert*; col. 9, lines 62-68)(emphasis added). Thus, it is the computer 60 that verifies the countersign. There is simply no teaching or suggestion that the countersign is presented to the user for the user's evaluation, and for the user to provide an indication that the countersign (or any other secret code) is correct.

Boerbert fails to disclose or suggest that after receiving an indication that the presented read secret code is correct, a biometric feature presented by the user is read. While Boerbert notes that "in an alternate embodiment, user authentication device 72 could include a biometric device for determining a unique physical attribute of user 23 such as fingerprints, palmprints or retinal pattern. That data would then be sent to computer 60 during the user verification process described in FIG. 4" (*Boerbert*; col. 41-46), no teaching or suggestion is provided that such a physical attribute or biometric feature is read after requiring the user to enter an indication that a secret code, read from a data carrier and then displayed for the user's evaluation, is correct.

According to the present invention, a user authentication scheme employs the use of a biometric feature. However, prior to reading a user's biometric feature, the user is required to recognize and respond to a secret code, known only to the rightful user, which is stored on a data carrier presented during the course of the authentication. Thus, a data carrier terminal reads the secret code from the data carrier, and then presents (displays) the secret code to the user for the user to evaluate and recognize, and only upon the user's indication that the secret code is correct does the authentication process proceed with reading, and evaluation, of the biometric feature. By this method, the data carrier terminal may be authenticated since only an authentic data carrier terminal will be able to properly decrypt and display the secret code for the user's recognition.

Such an authentication scheme differs from that disclosed by Boerbert, and Boerbert fails to disclose each and every element set forth in claim 1. Accordingly, it is respectfully submitted that Boerbert fails to form a prima facie case of obviousness of claim 1 and therefore claim 1 and claims 2 and 3 which depend from claim 1 are allowable.

Claims 4 and 7 recite a data carrier, and an authentication system, respectively, wherein a data carrier comprises a first memory area in which a secret code is stored such that the secret code can be read, decrypted, ***and displayed*** only by an authorized data carrier terminal to authenticate the data carrier terminal.

As discussed above, Boerbert does not disclose or suggest that a secret code is read from a data carrier ***and then displayed*** to the user. Accordingly, Boerbert fails to disclose or suggest each and every element set forth in claims 4 and 7 since each of these claims require that the secret code stored on the data carrier be read, decrypted, ***and displayed*** by a data terminal in order to authenticate the data terminal.

Therefore, it is respectfully submitted that Boerbert fails to form a prima facie case of obviousness of claims 4 and 7, and their respective dependent claims 5-6 and 8-9.

For at least these reasons, it is respectfully submitted that all of claims 1-9 are allowable over Boerbert. Accordingly, withdrawal of the rejection is respectfully requested.

Conclusion

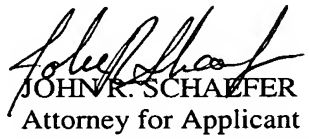
In view of the amendments to the claims, and in further view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-9 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date: September 28, 2006



JOHN R. SCHAEFER
Attorney for Applicant
Registration No. 47,921